Remarks

This is a submission accompanying the filing of a RCE request in response to the Office Action dated March 14, 2005.

Per the above amendment, claims 1, 2, 3, 4, 5, 6, 15, and 16 have been amended and claims 8-14, 17, and 19-22 canceled.

In the March 14 Office Action, Funakoshi et al (US Patent 6,401,207) and Eyer et al (US Patent 5,485,577) were the main references relied upon and combined by the examiner for rejecting the claims as being obvious.

The feature of the claimed inventions is that a reference table (in a memory 4) stores a plurality of predetermined key generation algorithms, and the one algorithm which should be used can be identified from among the predetermined key generation algorithms in response to algorithm identification information (an algorithm number in the embodiment of this invention) by referring to the reference table.

In the embodiment of this invention, the key generation algorithm used by the key generator 1 in the primary section P is selected from among a plurality of predetermined key generation algorithms. The reference table in the memory 4 in the secondary section Q stores all the predetermined key generation algorithms which can be used by the key generator 1. In the event that the used key generation algorithm is illegally disclosed, the key generation algorithm used by the key generator 1 is changed to another of the predetermined key generation algorithms and the updated algorithm identification information corresponding to the new key generation algorithm is transmitted from the primary section P to the secondary section Q. In this case, the new key generation algorithm is read out from the reference table in response to the transmitted algorithm identification information, and the key generator 5 in the secondary section Q properly operates in response to the new key generation algorithm.

Since the reference table storing all the predetermined key generation algorithms is provided in the secondary section Q, the key generation algorithm used in the secondary section Q can be updated in accordance with the change of the key generation algorithm used in the primary section P, provided that the algorithm identification information is transmitted from the primary section P to the secondary section Q. Specifically, when the key generation algorithm used in the primary section P is changed to a new one, the updated algorithm identification information for identifying the new key generation algorithm is transmitted from the primary section P to the secondary section Q. The transmitted algorithm identification information allows the secondary section Q to identify the new algorithm from among the predetermined key generation algorithms in the reference table. Thus, the secondary section Q uses the identified key generation algorithm, that is, the new key generation algorithm.

In Funakoshi et al (US Patent 6,401,207), an authentication key generating portion 15 generates an authentication key by encoding the seed in accordance with a predetermined algorithm (column 2, lines 65-66). Specifically, an authentication key generating portion 15 encodes the seed SEED in accordance with a predetermined encoding algorithm to generate an authentication key KEYCHK (column 6, lines 9-13). Furthermore, a key generating portion 22 encodes the received seed SEED by the use of an encoding algorithm as same as the encoding algorithm that is used when the authentication key generating portion 15 generates the key KEY (column 6, lines 58-62).

Funakoshi et al do not teach the reference table and the algorithm identification information set forth in the claimed inventions. Therefore, in the system of Funakoshi et al, in the event that the encryption algorithm used in the KEY UNIT 2 is illegally disclosed, if the encryption algorithm used in the ECU 1 is changed to new one, it is difficult to transmit information about the new encryption algorithm to the KEY UNIT 2 and to change the encryption algorithm used by the KEY UNIT 2 to a corresponding new one.

Eyer et al (US Patent 5,485,577) do not teach the reference table and the algorithm identification information in the claimed inventions.

Funakoshi et al and Eyer et al in combination therefore fail to teach the above-mentioned feature of the claimed inventions. The claimed inventions are therefore patentably distinguishable over Funakoshi et al and Eyer et al.

Respectfully submitted,

Louis Woo, RN 31,730
Law Offices of Louis Woo
717 North Fayette Street
Alexandria, VA 22314
(703) 299-4090

Date: June 9 2005